EXHIBIT 7

HOSIE | RICE LLP
ATTORNEYS AT LAW

Transamerica Pyramid, 34th Floor
600 Montgomery Street
San Francisco, California 94111
T: 415.247.6000 F: 415.247.6001

February 2, 2011

VIA E-MAIL AND U.S. MAIL

Christopher O. Green
Fish & Richardson
1180 Peachtree Street NE, 21st Floor
Atlanta, GA 30309
cgreen@fr.com

Re: *Rule 408 Settlement Communication – For Settlement Purposes Only*
Implicit Networks v. Hewlett-Packard Company

Dear Chris:

As I promised in our call yesterday, this is the first of two letters conveying information that HP may wish to consider in advance of the mediation, now confirmed for March 7, 2011.

Attached hereto is the preliminary infringement report prepared by Implicit's expert, David Bernstein.

The second letter, which I hope to get out tomorrow, will address the various inequitable conduct allegations raised in the defendants' amended answers, filed two weeks ago.

Very truly yours,

Spencer Hosie

Enc.

Cc: Kathi Lutton (w/enc.)

Internal Notes

Regarding the matter of

US Patents 6,629,163 and 7,711,857
And Hewlett-Packard

Prepared for Hosie Rice LLP

by

David Bernstein

Independent Consultant
Cloud Strategy Partners, LLC

Table of Contents

Introduction

I have been retained by Hosie Rice LLP in a matter related to US Patents 6,629,163 and 7,711,857 and HP. In addition to the patents themselves I've used publically available documents and I was asked study all of these with respect to infringement of various HP products.

These are my internal notes and are not meant to be a formal report of any kind.

Here's the behavior I am looking for:

- Non-predefined sequence of components
- for processing each message
- based on the first packet of the message
- so that subsequent packets of the message
- can be processed without re-identifying the components,
- wherein different non-predefined sequences of components
- can be identified for different messages,
- each component being a software routine,
- and wherein dynamically identifying includes selecting individual components
- to create the non-predefined sequence of components
- and for each packet of each message
- performing the processing of the identified non-predefined sequence of components of the message
- wherein state information generated by performing the processing of a component for a packet
- is available to the component
- when the component processes the next packet of the message.

HP Products Studied

HP has a broad networking product line which is largely a result of the 3Com acquisition. Specifically, I am looking at three areas for HP:

1. **HP L2/L3 Switches, and HP Routers**. These will contain deep packet inspection based QoS mechanisms, which are notoriously infringing on '163. These systems infringe as follows. Once can specify, while the system is running, a definition of a flow. This is not build-time or precompiled functionality, it is dynamic. One defines the policies, which are usually complicated enough in themselves to be like programming, and one defines actions. So once this is bound

into the running system, the system starts looking at the packets. There is a packet inspection capability used to identify a particular flow; once it finds a flow (usually in the first packet), it processes that flow differently in the machine from there out. Sometimes it will change this traffic so something differ happens downstream – the arranging of the editing component to change the traffic is an example of a dynamic component. Sometimes it will arrange different output queuing modules to process downstream – that's a dynamic component. One can arrange a pile-on of policies and actions, and they execute in a pipeline, on after another. Sometimes the actions of one effect the actions of another. In any case, if after a packet classification, I see a flow which is now handled by different modules which are arranged to act on the flow to implement the QoS, that's '163 infringing, as far as typical QoS goes.

2. **HP Security Devices**, in particular, Intrusion Prevention Systems / Threat Management Systems (IPS/TMS). Same idea here, these systems can dynamically accept programming which defines what a threat is. It's usually very rich; a combination of "filter packs" and "virus signatures" which are detailed instructions to the machine as to how to recognize traffic of a certain character. From there, the flow is identified, and the security administrator has defined what they want to happen to this traffic. It may be as simple as arranging for a "drop packets" component or "rate limit" component to be put in place. But it can be much more complicated, as the traffic may already have started to escape that box, so the box must inform downstream boxes what to do. In this case, the IPS/TMS systems are acting in a coordinated way, the downstream boxes serve as processing components for the upstream detection component. One box, or system of boxes, both scenarios apply; if at first there is the classification of the suspected or identified traffic, the pipelined processing thereof, and then the arrangement of processing components downstream, this is infringing on '163.

3. **HP Application Services,** such as WAN acceleration, or load balancers. These devices always have a processing pipeline after a deep packet inspection. I believe HP's devices in these areas are not based on their own technologies however, they use partner solutions on their modular hardware. Will investigate.

Conclusions, Summary

HP L2/L3 Switches and HP Routers Infringe due to their QoS mechanisms

When one analyzes the HP L2/L3 switches, and the HP Routers, one can focus on the QoS mechanism to find a deep packet inspection driven system. The switches implement a classic QoS system:

1. If one desires to use QoS, policies and actions must be defined. These are programmed into the running switch with no reboot required.
2. The switch can use many different mechanisms to identify a traffic flow. All traffic flows are identified based on first packet inspection.
3. The first packet, as well as the rest of the flow, is then subject to the actions specified.
4. The packet inspection can leverage several pre-configured categorization based flow identification (ACL), or it can leverage what HP calls "Classification" based flow identification.
5. As HP puts it "By using classifier-based QoS, you can configure multiple match criteria that search multiple fields in packet headers to select the exact traffic you want". There is infinite flexibility as to the multiple-attribute match criteria one can use.
6. Once a flow is identified, by a match on the first or first few packets, the traffic is "marked" (re-written). One can specify the marking technique used, depending on the specific actions needed downstream. Marking is a method for carrying state information to the later components in the processing pipeline.
7. For "packets moving through the switch", certain types of marking is used. For "packets that are sent to downstream devices", other types of marking are used.
8. In the case of downstream devices, one can later configure downstream devices to read and use the [particular marking chosen.
9. "Classifier-based service policies (such as QoS, ..) share the same hardware resources with other software features". Resources in the switch are dynamically allocated for classifier based QoS services; if one specifies a system-consuming number of these, one can re-prioritize current resource usage by tuning down the classifier-based service policy software features to free the resources. In other words, the classifier-based service policy components are dynamically arranged for execution based on run time specified behavior, and based on the number of actual traffic streams in use.

As explained in the introduction, this behavior directly infringes on the technology specified in '163.

The routers are quite similar in their overall approach to QoS but a router has much more processing capability than a switch. Switches are not supposed to drop packets; their QoS capabilities are priority based (packet re-ordering perhaps) and marking of traffic for variable handling later. However, a router can apply many different QoS policies, including those which drop packets, causing "backpressure", and applying many different policies through output queue management.

Different types of routers use different algorithms for implementing these scenarios and sequence the algorithms and techniques into a component processing pipeline in order to effect the traffic differently. HP routers use several techniques including multiple queue handling, and a scheduling/prioritization mechanism based on "tokens". It is illustrative to see this in the

following diagram of a router components pipeline, taken from http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02639610/c02639610.pdf :

Figure 4 QoS processing flow

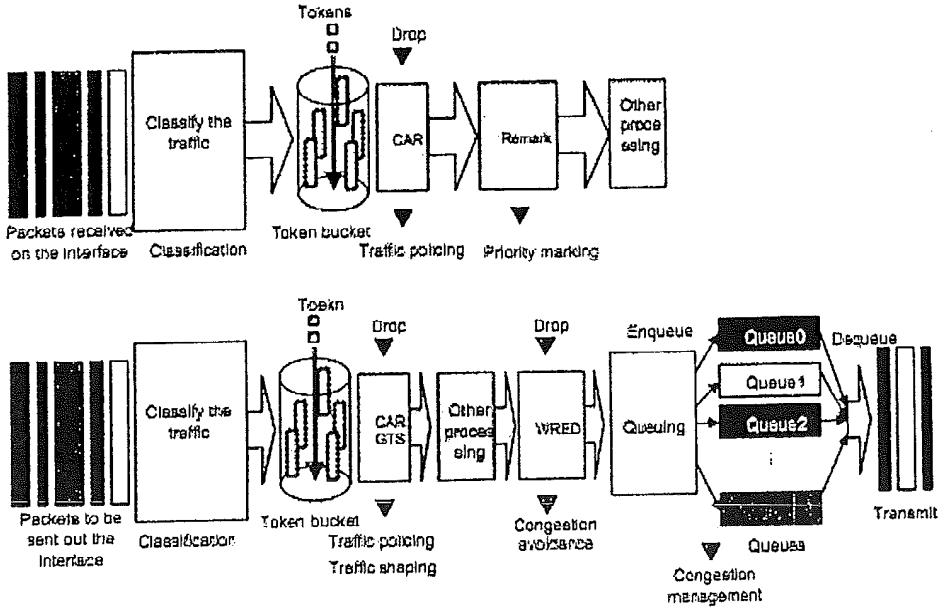


Figure 4 briefly describes how the QoS module processes traffic:

1. Traffic classifier identifies and classifies traffic for subsequent QoS actions.
2. The QoS module takes various QoS actions on classified traffic as configured, depending on the traffic processing phase and network status. For example, you may configure the QoS module to perform traffic policing for incoming traffic, traffic shaping for outgoing traffic, congestion avoidance before congestion occurs, and congestion management when congestion occurs.

Here one can clearly see, through the indicated color coding, that the traffic is processed in different parts of the pipeline, depending on the classification, the policies, and the specified actions.

It is not needed to detail here the extensive set of options in the processing and queuing. However, to step through the architecture of the system:

1. Just as with a switch, if one desires to use QoS, policies and actions must be defined. These are programmed into the running router with no reboot required.

2. The router can use many different mechanisms to identify a traffic flow. All traffic flows are identified based on first packet inspection.
3. The first packet, as well as the rest of the flow, is then subject to the actions specified.
4. The packet inspection can leverage several pre-configured categorization based flow identification, like the ACL's of the switch, but the routers contain Extended ACL definitions (EACL), or it can leverage what HP calls "Deep Application Recognition (DAR)" based flow identification. The Deeper Application Recognition (DAR) feature identifies packets of dynamic protocols like BitTorrent, HTTP, FTP, and RTP by examining Layer 4 to Layer 7 content other than the IP header.
5. "DAR can limit, block, or manipulate identified application traffic depending on your configuration."
6. DAR uses loadable "signature files". These are ".mtd" files. You place these files in a specified location on the running router and through management interfaces direct the system to load this file. Now, the router can recognize the new protocol and apply QoS to flows of that protocol.
7. "To apply QoS policies to data streams, to set packet priority or allocate bandwidth for example, use DAR to classify the data streams first".
8. As with the switch, you can configure multiple match criteria select the exact traffic you want. There is infinite flexibility as to the multiple-attribute match criteria, and also with DAR, one can use.
9. Once a flow is identified, by a match on the first or first few packets, there are many actions the router can perform, from "marking" as with the switch, to very complicated queue management.
10. As indicated by the diagram, the various processing components are arranged in a pipeline and state, in the form of marking, tokens, or other techniques, tells the components in the pipeline what processing to do on the flow.
11. Service policies (such as QoS, ..) using ACL, EACL, and DAR share the same hardware resources with other software features. Resources in the router are dynamically allocated for these QoS services; if one specifies a system-consuming number of these, one can re-prioritize current resource usage by tuning down the service policy software features to free the resources. In other words, the service policy components are dynamically arranged for execution based on run time specified behavior, and based on the number of actual traffic streams in use.

As explained in the introduction, this behavior directly infringes on the technology specified in '163.

HP Tipping Point Security Systems Infringe due to their IPS mechanisms

HP has a set of security devices which are the "TippingPoint" brand. This system is both an in-line system (Intrusion Prevention) as well as an out-of-band (Intrusion Detection) system [where one system detects the intrusions, and directs other systems to actually do the prevention]. The TippingPoint system is quite dynamic and programmable, and is driven by deep packet inspection through and though. As the datasheet on http://www.computerlinks.com/FMS/173090.pdf says:

1. The TippingPoint system is programmed, while it is running, by loading various "multiple IPS filter packs, security services, and additional partner security solution integrations".
2. It has a configuration system which allows administrators to load complicated policies into it, if the default configurations are to be customized.
3. It also supports automatic traffic characterization through "Sophisticated algorithms baseline normal traffic, allowing for automatic thresholds and throttling of malicious or unwanted application traffic"
4. Traffic first enters the TippingPoint and it performs Deep Packet Inspection "Through a combination of pipelined and massively parallel processing hardware, the Threat Suppression Engine is able to perform thousands of checks on each packet flow simultaneously at Layers 2-7"
5. These streams are handed down the "pipelined processing" where components of several kinds are applied to the traffic.
6. Components are dynamically loaded from customer-defined IP reputation services, the TippingPoint Reputation Digital Vaccine (DV) Online Service, TippingPoint Web Application DV, data leakage protection (filter sets), location-based policies (perimeter, core...) and customer developed filter sets using the TippingPoint Custom Shield Writer (CSW).
7. The TippingPoint system will block identified threats.
8. It "also enables traffic classification and rate shaping", providing user-defined programming of friendly traffic rates and priorities, if those capabilities have been directed to be used by the network administrator.
9. In a large network, the TippingPoint core system can direct satellite TippingPoint systems to arrange for their enforcement processing components to be activated, in downstream network segments. State information about traffic flows are communicated from the core system to the downstream systems.

As explained in the introduction, this behavior directly infringes on the technology specified in '163.

HP Applications Services Infringe due to Citrix or Riverbed software used – but not clear if this is HP's problem – they just make the hardware blade, and you buy the software separately. Don't know if that makes HP need a license

HP has a hardware blade, which allows for in-line traffic to be re-directed to software running on that blade, which can be provided by a third party. They have several third parties who have adapted their network-based software to this blade, including Citrix NetScaler (load balancer), and Riverbed 9WAN optimization). We know from previous analysis that these technologies in and of themselves infringe on '163.

As far as I can tell, HP does not directly sell these modules. As the title of this section indicates, I am not sure if this is HP's problem or not.

Backup Info, Cut and Paste references

What follows are some salient points I got from HP documents which helped me arrive at my conclusions.

QoS – HP L2/L3 Switches, and HP Routers

HP L2/L3 Switches

From
http://h10144.www1.hp.com/customercare/support/manuals/usermanuals/k.14.52/wwhelp/wwhimpl/js/html/wwhelp.htm

Layer 2 802.1p Prioritization

In classifier-based packet classification, match criteria provide a way to select the packets on which you want to execute QoS actions, such as rate-limiting or 802.1p prioritization. Match criteria are configured by creating a class of IPv4 or IPv6 traffic, which contains one or more match or ignore statements. A traffic class may be used by any classifier-based software feature, such as QoS or port mirroring.

By using classifier-based QoS, you can configure multiple match criteria that search multiple fields in packet headers to select the exact traffic you want to rate-limit or prioritize for a port or VLAN interface. A classifier-based QoS policy is especially useful when you want to manage different types of traffic in the same way (for example, to prioritize both IP subnet and voice traffic).

As described in "QoS Operation" on page 6-9, when you apply or reconfigure QoS actions for selected packets, QoS supports different types of traffic marking

By setting a new 802.1p priority value, QoS allows you to control the priority of outbound packets moving through the switch.

Layer 3 DSCP Marking

By changing or honoring the settings of the DSCP codepoint in IP packet headers, QoS allows you to control the DSCP and associated 802.1p priority values in outbound IP packets that are sent to downstream devices.

You can later configure downstream devices to read and use the DSCP policy that QoS sets. When marking the DSCP bits in IP packets,

VLAN and Untagged VLAN Environments

QoS operates in VLAN-tagged and untagged environments. If your network does not use multiple VLANs, you can still implement the 802.1Q VLAN capability to allow packets to carry an 802.1p priority to the next downstream device

Classifier-Based Traffic Marking

Classifier-based per-port or per-VLAN QoS policies support the following traffic-marking actions. Note that in addition to globally-configured QoS traffic marking (802.1p and DSCP prioritization), classifier-based QoS policies also support IP precedence and rate-limiting.

Layer 2 802.1p prioritization: Controls the outbound port queue priority for traffic leaving the switch, and (if traffic exits through a VLAN-tagged port) sends the priority setting in packet headers to downstream devices.
Layer 3 IP precedence-bit marking: Enables the switch to set, change, and honor prioritization policies by using the IP precedence bits in the ToS byte of IPv4 packet headers and Traffic Class byte of IPv6 headers.
Layer 3 DSCP marking: Enables the switch to set, change, and honor prioritization policies by using the Differentiated Services (diffserv) bits in the ToS byte of IPv4 headers and Traffic Class byte of IPv6 headers.
Rate-limiting: Enables a port or VLAN interface to allow only the specified amount of bandwidth to be used for inbound traffic. When traffic exceeds the configured limit, it is dropped.

Using Match Criteria

To identify the packets that belong to a traffic class for further processing by policy actions, use **match** and **ignore** commands in a class configuration:

match commands define the values that header fields must contain for a packet to belong to the class and be managed by policy actions.

ignore commands define the values which, if contained in header fields, exclude a packet from the policy actions configured for the class. An ignored packet is transmitted without having a policy action performed on it.

Match/ignore statements compare the values in packet fields with specified criteria in the sequential order in which the statements are entered in the class, until a match is found. Be sure to enter match/ignore statements in the *precise order* in which you want their criteria to be used to check packets.

As soon as a field in a packet header matches the criteria in a **match** statement, the sequential comparison of match criteria in the class stops, and the policy actions configured for the class are executed on the packet.

Checking Resource Usage

After you apply a service policy to an interface, use the **show policy resources** command to verify the amount of additional resources used and the amount of resources that are still available on the switch. Classifier-based service policies (such as QoS or mirroring) share the same hardware resources with other software features, such as ACLs, virus throttling, management VLAN, globally configured QoS policies, MAC-based mirroring policies, and so on.

Use the displayed information to decide if you need to re-prioritize current resource usage by reconfiguring or disabling software features to free the resources reserved for less important features.

HP Routers

From
http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02639610/c02639610.pdf

Figure 3 Position of the QoS techniques in a network

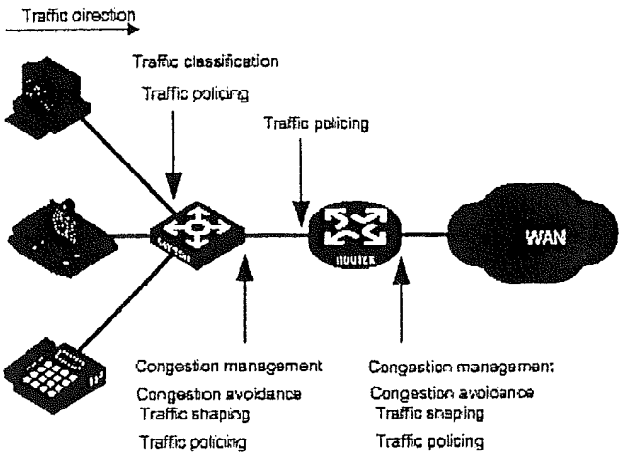


Figure 4 QoS processing flow

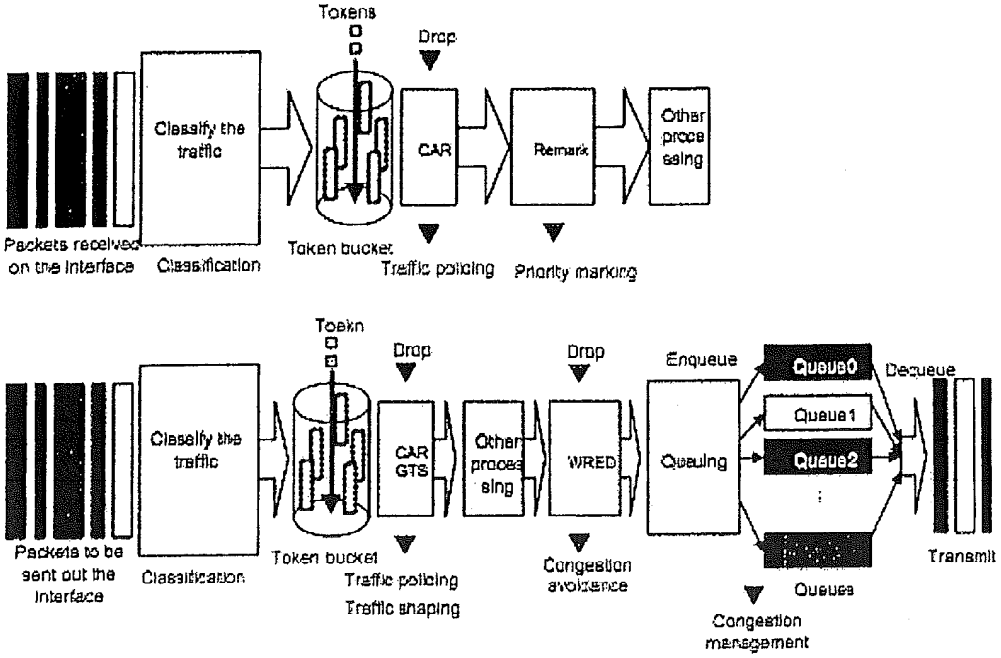


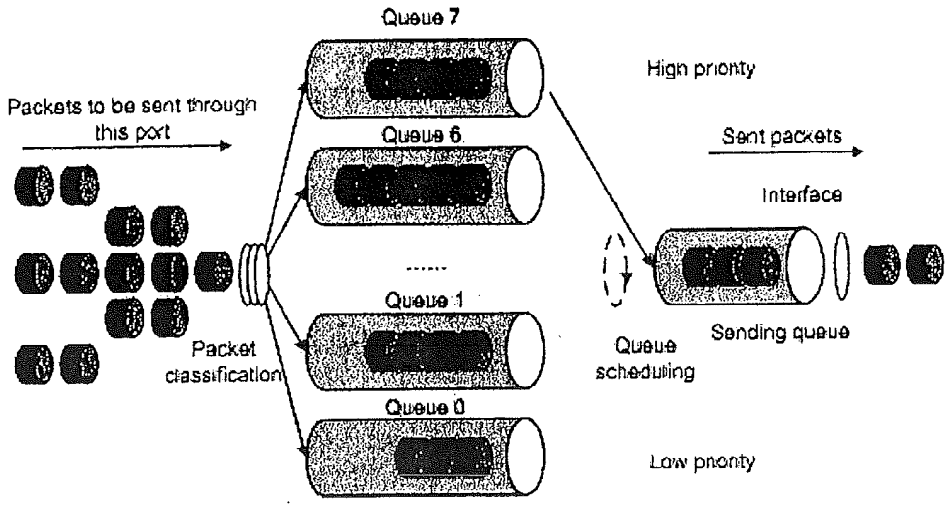
Figure 4 briefly describes how the QoS module processes traffic:

1. Traffic classifier identifies and classifies traffic for subsequent QoS actions.
2. The QoS module takes various QoS actions on classified traffic as configured, depending on the traffic processing phase and network status. For example, you may configure the QoS module to perform traffic policing for incoming traffic, traffic shaping for outgoing traffic, congestion avoidance before congestion occurs, and congestion management when congestion occurs.

SP queuing

SP queuing is specially designed for mission-critical applications, which require preferential service to reduce the response delay when congestion occurs.

Figure 7 Schematic diagram for SP queuing



As shown in Figure 7, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

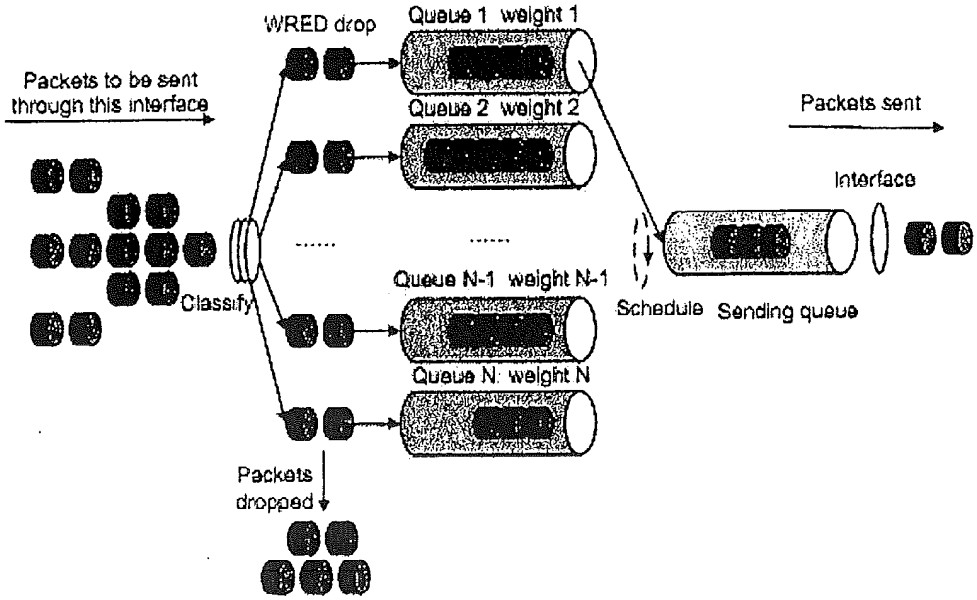
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. Thus, you can assign mission-critical packets to the high priority queue to ensure that they are always served first and common service packets to the low priority queues and transmitted when the high priority queues are empty.

The disadvantage of SP queuing is that packets in the lower priority queues cannot be transmitted if there are packets in the higher priority queues. This may cause lower priority traffic to starve to death.

Relation between operation of WRED and queuing

The relation between WRED and queuing mechanism is shown in the following figure:

Figure 10 Relationship between WRED and queuing mechanism



Introduction to DAR

The Deeper Application Recognition (DAR) feature identifies packets of dynamic protocols like BitTorrent, HTTP, FTP, and RTP by examining Layer 4 to Layer 7 content other than the IP header. The feature helps service providers and businesses limit aggressive bandwidth use by applications like BitTorrent to ensure fairness and network performance.

BitTorrent is a peer to peer (P2P) file sharing communications protocol, which enables personal computers to directly exchange data or services. P2P has been widely used for content (such as audio and video) file sharing, representing a large amount of bandwidth on the Internet.

DAR can limit, block, or manipulate identified application traffic depending on your configuration.

Configuring BT traffic limiting

BitTorrent (BT) is a kind of shared software used for file downloading. It features the more users, the faster the downloading. Though BT reduces the load of the download server, it greatly increases the amount of downloaded data, occupying a large amount of network bandwidth and serious affecting other network applications. Thus, controlling BT traffic is required.

QoS identifies BT traffic by the BitTorrent protocol field, and then limits BT traffic.

This is an optional procedure to configure BT traffic limiting:

1. Enter system view:

   $>system-view

2. Enter advanced ACL view:

   $>acl number *acl-number* [**match-order** { **config** | **auto** }]

3. Define an ACL rule:

   $>rule [*rule-id*] **permit tcp** [*rule-string*]

4. Exit ACL view:

   $>quit

5. Enter class view:

   $>traffic classifier *tcl-name*

6. Configure an ACL based match criterion:

   $>if-match acl *acl-number*

7. Match BT packets:

   $>if-match protocol bittorrent

8. Exit class view:

   $>quit

9. Enter traffic behavior view:

   $>traffic behavior *behaviorname*

10. Configure a CAR action:

    $>car cir *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size* [**red** *action*]

IPS – HP Security Devices

HP TippingPoint IPS systems

From
http://h10163.www1.hp.com/products_ips.html

The TippingPoint IPS is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious.

The system is built upon TippingPoint's Threat Suppression Engine (TSE) - a highly specialized hardware-based intrusion prevention platform consisting of state-of-the-art network processor technology and TippingPoint's own set of custom ASICs. The TippingPoint ASIC-based Threat Suppression Engine is the underlying technology that has revolutionized network protection. Through a combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The TSE architecture utilizes custom ASICs, a 20 Gbps backplane and high-performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with a latency of less than 84 microseconds, independent of the number of filters that are applied.

The TippingPoint TSE architecture also enables traffic classification and rate shaping. Sophisticated algorithms baseline "normal" traffic allowing for automatic thresholds and throttling so that mission critical applications are given a higher priority on the network.

The integral part of the TippingPoint solution is the Digital Vaccine® Service. Developed by TippingPoint's world-renowned security researchers (DVLabs), the Digital Vaccine service delivers comprehensive security filters to TippingPoint Intrusion Prevention Systems to to pre-emptively protect against the exploit of new and zero-day vulnerabilities. These filters, created to block multiple attack variants on a single vulnerability versus a simple exploit, provide attack recognition accuracy without compromising network performance. Digital Vaccine updates are automatically delivered twice a week, or immediately when critical vulnerabilities and threats emerge

The network security and data center protection provided by TippingPoint's IPS N-Platform includes an Extensible Security Framework which has a modular software design built to support faster development and deployment of new:

- IPS filter packages
- Security services
- Partner security solution integrations

Threat Suppression Engine

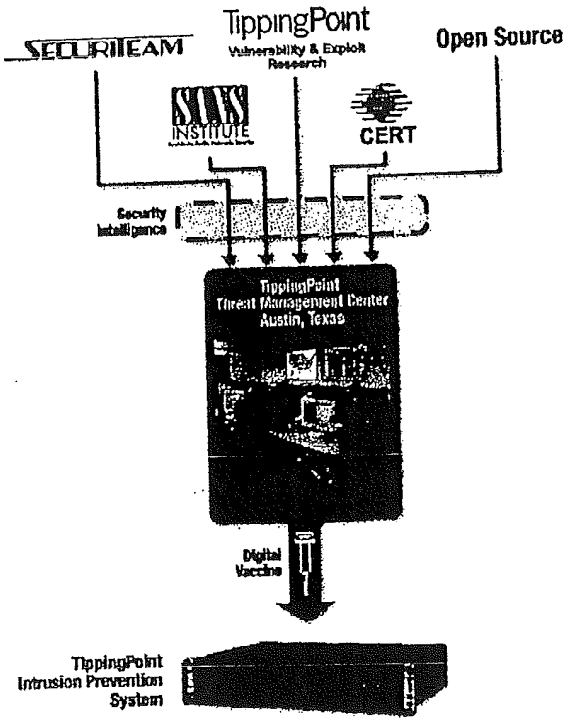
The Threat Suppression Engine employed by the TippingPoint IPS N-Platform is designed to keep pace with the changing and quickly increasing threats, and the evolving demands of today's enterprise network security and data center protection needs. Benefits of the new TSE include:

- Increased deep packet inspection capacity from additional parallel processing
- Greater threat protection to handle years of future threats
- Run multiple IPS filter packs and security services simultaneously

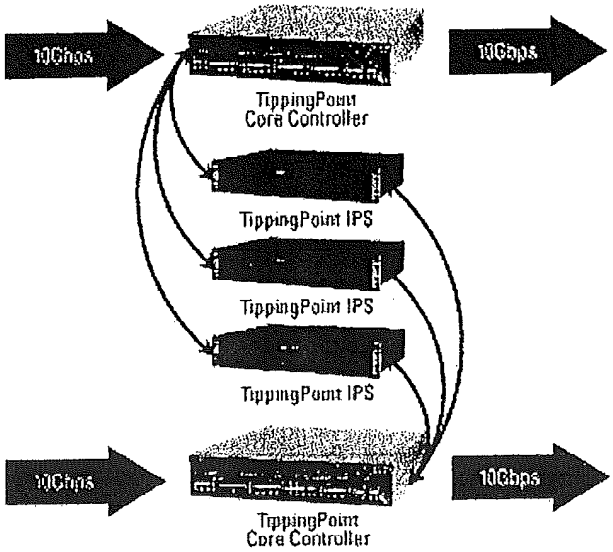
From
http://h10163.www1.hp.com/products_dv.html

TippingPoint DVLabs security team simultaneously develops new attack filters to address the vulnerabilities and incorporates these filters into Digital Vaccines. Vaccines are created not only to address specific exploits, but also potential attack permutations, protecting customers from Zero-Day threats. For maximum security coverage, TippingPoint deploys a variety of security filters, including traffic anomaly filters and vulnerability-based filters. In the case of a virus, where there is no underlying vulnerability, TippingPoint delivers attack signatures.

New filters are continuously fed to the IPS to keep it up-to-date against the latest vulnerabilities. Each filter can be thought of as a Virtual Software Patch that is created within the network to protect downstream hosts from attack.



The TippingPoint Core Controller is deployed as a 'bump-in-the wire' network element for up to three 10Gbps network links. Traffic entering the Core Controller is intelligently flow balanced to a bank of TippingPoint IPS's where traffic inspection and enforcement are performed. Malicious and unwanted traffic is blocked, and clean traffic is returned to the Core Controller for distribution to the appropriate 10Gbps egress link, allowing organizations to scale security traffic inspection and enforcement.



Application Networking Services – HP Services Module

HP Advanced services zl Module Integrated applications

Application Delivery platforms and solutions

The HP application delivery portfolio provide the capability to host best in class AllianceONE applications in the areas of Security, Mobility, UC&C, and Infrastructure on the HP 5400zl and 8200zl Chassis.

Services zl Module series

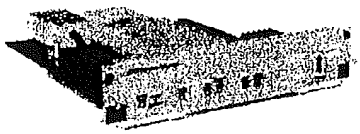
Platforms
- Services zl Module
- Advance Services zl Module

Solutions
- Session Border Controller zl Module with Avaya Aura™ Session Border Controller Application
- Extended Services zl Module with Riverbed® Steelhead RiOS® Application

AllianceONE: Networking Specialization
- AllianceONE

Advanced services zl Module integrated applications
- Citrix NetScalar
- NetScout nGenius Integrated Agent

Services zl Module integrated applications
- InMon Traffic Sentinel
- Fortinet Fortigate Security Appliances
- AirTight Spectra Guard Enterprise
- .vantronix Firewall ZL1 .vFW-ZL1
- .vantronix Router .vRT-ZL1
- Aastra 5000
- Aastra MX-ONE
- VBrick VIP
- Ekahau Positioning Engine
- Riverbed Technology WAN Optimization



Key features

- High-performance compute platform
- Environment for ProCurve ONE applications
- Two 10-GbE connections to the switch backplane
- Industry-leading warranty

Datasheet

HP ProCurve ONE Services zl Module

Part of the HP ProCurve ONE Program that enables secure best-in-class applications and services in the ProCurve infrastructure, the HP ProCurve ONE Services zl Module is a x86-based server module that provides two 10-GbE network links into the switch backplane. Coupled with ProCurve-certified services and applications that can take advantage of a switch-targeted API for better performance, this module creates a virtual appliance within a zl switch slot to provide solutions for business needs, such as network security. This services module can be moved to any zl switch in the environment.

WAN Acceleration is delivered by Riverbed technology, on this add-on card hardware from HP

Load Balancing is delivered by Citrix, on this add-on card hardware from HP

» Overview | » Features | » Benefits | » Components | How to Buy

HP Networking integrated applications are available for purchase from Citrix or channel partners of the Citrix.

EXHIBIT 8

SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
GEORGE F. BISHOP (CA Bar No. 89205)
gbishop@hosielaw.com
DIANE S. RICE (CA Bar No. 118303)
drice@hosielaw.com
WILLIAM P. NELSON (CA Bar No. 196091)
wnelson@hosielaw.com
HOSIE RICE LLP
Transamerica Pyramid, 34th Floor
600 Montgomery Street
San Francisco, CA 94111
(415) 247-6000 Tel.
(415) 247-6001 Fax

Attorneys for Plaintiff
IMPLICIT NETWORKS, INC.

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IMPLICIT NETWORKS, INC.,

Plaintiff,

v.

JUNIPER NETWORKS, INC.,

Defendant.

Case No. C 10-4234 SI

PLAINTIFF'S DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS

APPENDIX A

(Juniper Products Containing Infringing Technologies)

Application Acceleration Category

1. DX3200 Series Application Acceleration Platform (deprecated)
2. DX3250 Series Application Acceleration Platform (deprecated)
3. DX3280 Series Application Acceleration Platform (deprecated)
4. DX3600 Series Application Acceleration Platform (deprecated)
5. DX3650 / DX3650 FIPS Application Acceleration Platform (deprecated)
6. DX3670 Application Acceleration Platform (deprecated)
7. DX3680 Application Acceleration Platform (deprecated)
8. WX Stack Series Data Center Acceleration (deprecated)
9. WX 15 Series Application Acceleration Platform (deprecated)
10. WX 20 Series Application Acceleration Platform (deprecated)
11. WX 50 Series Application Acceleration Platform
12. WX 60 Series Application Acceleration Platform (deprecated)
13. WX 80 Series Application Acceleration Platform
14. WX 100 Series Application Acceleration Platform (deprecated)
15. WXC 250 Series Application Acceleration Platform (deprecated)
16. WXC 500 Series Application Acceleration Platform (deprecated)
17. WXC 590 Series Application Acceleration Platform
18. WXC 1800 Series Application Acceleration Platform
19. WXC 2600 Series Application Acceleration Platform
20. WXC 3400 Series Application Acceleration Platform
21. J2320 Series Router with ISM WXC 200 installed
22. J2350 Series Router with ISM WXC 200 installed
23. J4350 Series Router with ISM WXC 200 installed
24. J6350 Series Router with ISM WXC 200 installed
25. Junos Pulse

QOS Category

1. EX2200 Series Switches
2. EX2500 Series Switches
3. EX3200 Series Switches
4. EX4200 Series Switches
5. EX4500 Series Switches
6. EX8208 Series Switches
7. EX8216 Series Switches
8. QFX3500 Series Switches
9. CTP150 Series Circuit to Packet Platform
10. CTP1002 Series Circuit to Packet Platform
11. CTP1004 Series Circuit to Packet Platform
12. CTP1012 Series Circuit to Packet Platform
13. CTP2008 Series Circuit to Packet Platform
14. CTP2024 Series Circuit to Packet Platform

15. CTP2056 Series Circuit to Packet Platform
16. E120 Series Broadband Services Router
17. E320 Series Broadband Services Router
18. ERX310 Series Broadband Services Router
19. ERX705 Series Broadband Services Router
20. ERX710 Series Broadband Services Router
21. ERX1410 Series Broadband Services Router
22. ERX1440 Series Broadband Services Router
23. J2300 Series Router (deprecated)
24. J2320 Series Router
25. J2350 Series Router
26. J4300 Series Router (deprecated)
27. J4350 Series Router
28. J6300 Series Router (deprecated)
29. J6350 Series Router
30. LN1000 Series Mobile Secure Router
31. M5 Series Router (deprecated)
32. M7i Series Router
33. M10 Series Router (deprecated)
34. M10i
35. M20 Series Router (deprecated)
36. M40 Series Router (deprecated)
37. M40e Series Router
38. M120 Series Router
39. M160 Series Router (deprecated)
40. M320 Series Router
41. MX5 Series Router
42. MX10 Series Router
43. MX40 Series Router
44. MX80 Series Router
45. MX240 Series Router
46. MX480 Series Router
47. MX960 Series Router
48. T320 Series Router
49. T640 Series Router
50. T1600 Series Router
51. T4000 Series Router
52. TX Matrix Series Router
53. TX Matrix Plus Series Router

Security Category

1. J2320 Series Router
2. J2350 Series Router
3. J4350 Series Router
4. J6350 Series Router
5. LN1000 Series Mobile Secure Router

6. NetScreen-5200 Series
7. NetScreen-5400 Series
8. MX240 Series Router with Multiservices DPC installed
9. MX480 Series Router with Multiservices DPC installed
10. MX960 Series Router with Multiservices DPC installed
11. M7i Series Router with Multiservices PIC installed
12. M10i Series Router with Multiservices PIC installed
13. M40e Series Router with Multiservices PIC installed
14. M120 Series Router with Multiservices PIC installed
15. M320 Series Router with Multiservices PIC installed
16. T320 Series Router with Multiservices PIC installed
17. T640 Series Router with Multiservices PIC installed
18. T1600 Series Router with Multiservices PIC installed
19. TX Matrix Series Router with Multiservices PIC installed
20. IDP 10 Series Intrusion Detection and Prevention Appliance (deprecated)
21. IDP 50 Series Intrusion Detection and Prevention Appliance (deprecated)
22. IDP 75 Series Intrusion Detection and Prevention Appliance
23. IDP 100 Series Intrusion Detection and Prevention Appliance (deprecated)
24. IDP 200 Series Intrusion Detection and Prevention Appliance (deprecated)
25. IDP 250 Series Intrusion Detection and Prevention Appliance
26. IDP 500 Series Intrusion Detection and Prevention Appliance (deprecated)
27. IDP 600 C/600 F Series Intrusion Detection and Prevention Appliance (deprecated)
28. IDP 800 Series Intrusion Detection and Prevention Appliance
29. IDP 1000 Series Intrusion Detection and Prevention Appliance (deprecated)
30. IDP 1100C 1100F Series Intrusion Detection and Prevention Appliance (deprecated)
31. IDP 4500 Series Intrusion Detection and Prevention Appliance (deprecated)
32. IDP 6500 Series Intrusion Detection and Prevention Appliance (deprecated)
33. IDP 8200 Series Intrusion Detection and Prevention Appliance
34. ISG1000 Series Integrated Security Gateway with Optional IPS
35. ISG2000 Series Integrated Security Gateway with Optional IPS
36. SRX100 Series Services Gateway
37. SRX210 Series Services Gateway
38. SRX220 Series Services Gateway
39. SRX240 Series Services Gateway
40. SRX650 Series Services Gateway
41. SRX1400 Series Services Gateway
42. SRX3400 Series Services Gateway
43. SRX3600 Series Services Gateway
44. SRX5600 Series Services Gateway
45. SRX5800 Series Services Gateway

CERTIFICATE OF SERVICE

I, Jerry Shaw, am a citizen of the United States and am employed in the County of San Francisco, State of California. I am over the age of 18 years and am not a party to the within action. My business address is Hosie Rice LLP, Transamerica Pyramid, 34th Floor, 600 Montgomery Street, San Francisco, California, 94111.

On May 23, 2011, I served the following attached

PLAINTIFF'S DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS

via Federal Express at San Francisco, California, addressed to the following parties:

DAVID C. MCPHIE
dmcphie@irell.com
REBECCA L. CLIFFORD
rclifford@irell.com
Irell & Manella LLP
840 Newport Center Drive, Suite 400
Newport Beach, CA 92660-6324

MORGAN CHU
mchu@irell.com
JONATHAN S. KAGAN
jkagan@irell.com
IRELL & MANELLA LLP
1800 Avenue of the Stars, Suite 900
Los Angeles, CA 90067-4276

Attorneys for Defendant
Juniper Networks, Inc.

I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATED: May 23, 2011

/s/ Jerry Shaw
Jerry Shaw